What is claimed is:

1. A process for registering data in a data management system and identifying uses of the registered data by users, comprising:

creating a template comprising a plurality of elements, wherein each element is defined by an element size, a start position and an initial position;

receiving a source file from data owners;

creating a fingerprint for the source file by recording portions of the source file that correspond to each of the elements in the template;

storing the source file and fingerprint in a database; and

comparing unknown data files to the fingerprint stored in the database to determine whether the unknown data files are copies of any portion of the source file.

2. A process as claimed in claim 1, further comprising branding the source file.

3. A process as claimed in claim 2, wherein branding comprises:

receiving a user defined data block from a user, wherein the data block includes user defined information;

examining the source file to determine whether the source file contains a data block;

building a concatenated string from the data block information;

embedding the data block within the source file.

4. A process as claimed in claim 3, wherein the information contained in the data block includes any of the following: rights information, licencing information, a counter, key words, file attributes and mandatory compliance information.

5. A process as claimed in claim 4, wherein compliance information comprises any of the following group: identification information, age information, custodial information and other mandatory information required by law for image data.

6. A process as claimed in claim 3, further comprising:

verifying whether the source file currently exists in the system;

creating a fingerprint for the source file if the file is not stored in the data management database; and

storing the source file and the associated file fingerprint in the database.

7. A process as claimed in claim 2, wherein branding further comprises:

receiving a request to brand a source file from a user;

retrieving a preassigned encryption key for the user, wherein the encryption key is stored in the database in association with the source file;

verifying that the user requesting the branding of the source file is authorized to request the branding of the file;

rejecting the branding and notifying the file owner if the requesting user is not authorized to brand the file;

if the requesting user is authorized to request the branding, encrypting the data block utilizing the preassigned encryption key assigned to the user; and

embedding the encrypted data block into the source file; and

creating a fingerprint of the source file with the embedded data block.

8. A process as claimed in claim 1, wherein the data includes pixel values and a plurality of color values for each pixel, and wherein creating a fingerprint further comprises:

averaging color values for predefined portions of the source file.

9. A data management system for managing, reviewing, comparing and detecting data on a network, comprising:

a data management server;

a key generator;

a source print generator; and

a source print detector.

10. A data management system as claimed in claim 9, further comprising a data embedding system.

11. A data management system as claimed in claim 9, the source print detector further comprising:

a searching member, wherein the searching downloads unknown files to the data management server from the network; and

a comparison member, the comparison member includes a storage database, and is configured to review the unknown files and compare the unknown files to a set of source prints stored on the storage database.

12. A process of registering, monitoring and tracking uses of data registered in a data management system on a network, comprising:

creating a template comprising a plurality of elements, wherein each element is defined by an element size, a start position and an initial position;

receiving a source file from data owners;

creating a fingerprint file for the source file by recording portions of the source file that correspond to each of the elements in the template;

storing the source file and fingerprint in a database;

searching the network for unknown files;

downloading unknown files to a data management server;

recording portions of the unknown files that correspond to each of the elements in the template to create a fingerprint for the unknown file;

comparing the fingerprint of the unknown file to the fingerprint of the source file; and

assigning a probability matching level for the unknown file based upon the comparison results of the comparison between the fingerprint of the unknown file and the fingerprint of the source file.